REMARKS

The present application was filed on June 7, 2001 with claims 1 through 32. Claims 1 through 32 are presently pending in the above-identified patent application.

In the Office Action, the Examiner rejected claims 1, 10, 17, 22, 26-29, and 31-32 under 35 U.S.C. §102(b) as being anticipated by Thurrott (Paul Thurrott, "What's New in Windows 2000 RC2 Reviewed," http://www.winsupersite.com/reviews/win2k_rc2_whatsnew.asp), rejected claims 1, 7-10, 12, 17, 22, 26-29, and 31-32 under 35 U.S.C. §102 as being anticipated by or, in the alternative, under 35 U.S.C. §103(a) as obvious over Cromer et al. (United States Patent Number 6,021,493), rejected claims 2-3, 13-14, 18-19, and 23-24 under 35 U.S.C. §103(a) as being unpatentable over Cromer et al. in view of Sanders et al. (United States Patent Number 5,231,375) and further in view of Lam (United States Patent Number 6,140,923), rejected claims 3, 14, 19, and 24 under 35 U.S.C. §103(a) as being unpatentable over Cromer et al. in view of Minasi (Mark Minasi, "Mastering Windows NT Server 4," 6th edition, 1999, ISBN: 0782124453), rejected claims 4 and 5 under 35 U.S.C. §103(a) as being unpatentable over Cromer et al. in view of Pearce et al. (United States Patent Number 6,308,272), and rejected claims 6, 11, 15-16, 20-21, 25, and 30 under 35 U.S.C. §103(a) as being unpatentable over Cromer et al. in view of Sobell (Mark G. Sobell, "A Practical Guide to the UNIX System," 3rd edition, 1997, ISBN: 0805375651).

Independent Claims 1, 12, 17, 22, 31 and 32

Independent claims 1, 17, 22, and 31-32 were rejected under 35 U.S.C. §102(b) as being anticipated by Thurrott, and claims 1, 12, 17, 22, and 31-32 were rejected under 35 U.S.C. §102 as being anticipated by or, in the alternative, under 35 U.S.C. §103(a) as obvious over Cromer et al. Regarding claim 1, the Examiner asserts that Thurrott teaches monitoring a network connection and generating an alarm if the network connection is disconnected. Also, regarding claim 1, the Examiner asserts that even if disconnection of the remote computer system did not result in the generation of the alarm, it would have been obvious to one of ordinary skill in the art to implement such a modification.

Applicants note that Thurrott teaches that "a new ***visual cue*** has been added to *alert **the user*** when the machine is disconnected from the network." (Network Disconnect Cue section.) Thurrott teaches that a *visual cue alerts the user*. If a machine is not being used, a theft alarm must alert one or more people who are ***not*** users. Thus, a visual cue that alerts a user of a machine is unlikely to be effective as an alarm to alert one or more individuals to a theft, as would be apparent to a person of ordinary skill in the art. Thus, a person of ordinary skill in the art would not interpret the visual cue disclosed by Thurrott as an alarm for indicating a theft.

Applicants also note that Cromer is directed to a method for detecting when a computer system has been disconnected from a data transmission network that "includes providing a plurality of computer systems connected to a main computer system via a data transmission network, each of said plurality of computer systems having a network connector for communicating data with the main computer." (Col. 2, lines 39-46.) An alert message is sent "from the main computer to a *network administrator* only if it is determined that at least one of the plurality of computer systems is not connected to the network." (Col. 2, lines 52-55; emphasis added; see, also, col. 7, lines 31-54, and col. 9, lines 18-30.) Cromer, however, does not disclose or suggest generating an alarm in the *removed device*. Cromer, in fact, actually teaches away from the present invention by teaching to install an alarm outside of the protected device. Thus, a person of ordinary skill in the art would not look to modify the system disclosed by Cromer to incorporate an alarm *in the protected device*. Independent claims 1, 22, 31, and 32 require *generating an alarm in said removed device* if said network connection is disconnected. Independent claim 12 requires *generating an alarm in said removed device* if said response is not received within a predefined time interval. Independent claim 17 requires *generating an alarm in said removed device* if said signal is no longer received.

Thus, Thurrott and Cromer et al., alone or in combination, do not disclose or suggest generating an alarm in said removed device if said network connection is disconnected, as required by independent claims 1, 22, 31, and 32, do not disclose or suggest generating an alarm in said removed device if said response is not received

within a predefined time interval, as required by independent claim 12, and do not disclose or suggest generating an alarm in said removed device if said signal is no longer received and a theft detection mode is enabled, as required by independent claim 17.

Additional Cited References

Sander et al. was also cited by the Examiner for its disclosure of a device connected to a network by a network connection that produces an audible alarm signal in the device. Applicants note that Sanders teaches that,

> in accordance with the present invention, whenever data processing equipment or electronic equipment 1000 is disconnected from DCM 1020, ***theft detection and alarm system 1010 generates an alarm data signal*** which is transmitted to DCM 1020 and, optionally, ***theft detection and alarm system 1010 generates an alarm at its physical location***. In response to the data signal from theft detection and alarm system 1010, DCM 1020 transmits an alarm status code to CBX 1030. In response, the above-described applications program in CBX 1030 transmits the alarm status code to theft and alarm system monitor 1050 along with configuration information related to DCM 1020. Once again, theft and alarm system monitor 1050 utilizes the status information, including the DCM configuration information, as a retrieval key to access database 1060 and to retrieve information which relates to the disconnected equipment. Then, theft and alarm system monitor generates a report which identifies the particular equipment which was disconnected. The report may be printed at a terminal in a central location and/or may be printed at security location in the vicinity of the disconnected DCM and/or may be printed at a security dispatch location and so forth.
>
> In either case, whether DCM 1020 or data processing or electronic equipment 1000 is disconnected, theft detection and alarm system monitor 1050 can send a message, in a manner which is well known to those of ordinary skill in the art, to a security terminal and/or cause ***an alarm to be sounded in the area of the disconnected equipment*** and/or place a telephone call to a predetermined security location and/or transmit a predetermined message to an external loud speaker, using CBX 1030. Further, various such strategies could be implemented as various times during the day. For example, alarm generations in response to disconnect information may be disabled at theft alarm system monitor 1050 during the day and activated during the night or on the week-end when most thefts are expected to occur. Further, alarm generation in response to disconnect information may be disabled at theft alarm system monitor 1050 on an equipment or location basis to enable one to move equipment.
> (Col. 4, lines 26-68.)

Sanders, however, does not disclose or suggest generating an alarm in the *removed device*.

Thus, Sanders et al. do not disclose or suggest generating an alarm in said removed device if said network connection is disconnected, as required by independent claims 1, 22, 31, and 32, do not disclose or suggest generating an alarm in said removed device if said response is not received within a predefined time interval, as required by independent claim 12, and do not disclose or suggest generating an alarm in said removed device if said signal is no longer received, as required by independent claim 17.

Lam was also cited by the Examiner for its disclosure of motivation to combine Sanders and Cromer. Lam, however, does not address the issue of devices connected to a network.

Thus, Lam does not disclose or suggest generating an alarm in said removed device if said network connection is disconnected, as required by independent claims 1, 22, 31, and 32, does not disclose or suggest generating an alarm in said removed device if said response is not received within a predefined time interval, as required by independent claim 12, and does not disclose or suggest generating an alarm in said removed device if said signal is no longer received, as required by independent claim 17.

Minasi was also cited by the Examiner for its disclosure of assigning rights to users that grant or deny access to certain objects (resources) such as turning off a device. Applicants note that Minasi is directed to registry control in an operating system, user rights, and object permissions. Minasi does not address the issue of detecting the removal of a device connected to a network.

Thus, Minasi does not disclose or suggest generating an alarm in said removed device if said network connection is disconnected, as required by independent claims 1, 22, 31, and 32, does not disclose or suggest generating an alarm in said removed device if said response is not received within a predefined time interval, as required by independent claim 12, and does not disclose or suggest generating an alarm in said removed device if said signal is no longer received, as required by independent

claim 17.

Pearce was also cited by the Examiner for its disclosure of monitoring that is set to activate automatically in a passive manner. Applicants note that Pearce is directed to a "security system using a security detector associated with a personal computer attached to an existing data transmission network, where the personal computer is effective to detect security breaches and transmit an alarm." (See, Abstract.) Pearce does not address the issue of detecting the removal of a device connected to a network.

Thus, Pearce does not disclose or suggest generating an alarm in said removed device if said network connection is disconnected, as required by independent claims 1, 22, 31, and 32, does not disclose or suggest generating an alarm in said removed device if said response is not received within a predefined time interval, as required by independent claim 12, and does not disclose or suggest generating an alarm in said removed device if said signal is no longer received, as required by independent claim 17.

Sobell was also cited by the Examiner for its disclosure of using a password to perform administrative tasks. Applicants note that Sobell is a guide to a UNIX system. Sobell does not address the issue of detecting the removal of a device connected to a network.

Thus, Sobell does not disclose or suggest generating an alarm in said removed device if said network connection is disconnected, as required by independent claims 1, 22, 31, and 32, does not disclose or suggest generating an alarm in said removed device if said response is not received within a predefined time interval, as required by independent claim 12, and does not disclose or suggest generating an alarm in said removed device if said signal is no longer received, as required by independent claim 17.

<u>Dependent Claims 2-11, 13-16, 18-21 and 23-30</u>

Dependent claims 10 and 26-29 were rejected under 35 U.S.C. §102(b) as being anticipated by Thurrott, claims 7-10, 22, and 26-29 were rejected under 35 U.S.C. §102 as being anticipated by or, in the alternative, under 35 U.S.C. §103(a) as obvious over Cromer et al., claims 2-3, 13-14, 18-19, and 23-24 were rejected under 35 U.S.C.

§103(a) as being unpatentable over Cromer et al. in view of Sanders et al. and further in view of Lam, claims 3, 14, 19, and 24 were rejected under 35 U.S.C. §103(a) as being unpatentable over Cromer et al. in view of Minasi, claims 4 and 5 were rejected under 35 U.S.C. §103(a) as being unpatentable over Cromer et al. in view of Pearce et al., and claims 6, 11, 15-16, 20-21, 25, and 30 were rejected under 35 U.S.C. §103(a) as being unpatentable over Cromer et al. in view of Sobell.

Claims 2-11, 13-16, 18-21, and 23-30 are dependent on claims 1, 12, 17, and 22, respectively, and are therefore patentably distinguished over Thurrott, Sanders et al., Lam, Pearce et al., Minasi, Sobell, and Cromer et al. (alone or in any combination) because of their dependency from independent claims 1, 12, 17, and 22 for the reasons set forth above, as well as other elements these claims add in combination to their base claim.

All of the pending claims, i.e., claims 1-32, are in condition for allowance and such favorable action is earnestly solicited.

If any outstanding issues remain, or if the Examiner has any further suggestions for expediting allowance of this application, the Examiner is invited to contact the undersigned at the telephone number indicated below.

The Examiner's attention to this matter is appreciated.

Respectfully submitted,

Date: October 11, 2005

Kevin M. Mason
Attorney for Applicants
Reg. No. 36,597
Ryan, Mason & Lewis, LLP
1300 Post Road, Suite 205
Fairfield, CT 06824
(203) 255-6560